

ORTHOGONAL CIRCLES AND A FIXED-DIMENSIONAL SEPARATED-DISTANCE COUNTEREXAMPLE

JOHN TRIPODO

ABSTRACT. A finite set of points in Euclidean space is *distance-separated* if the lengths of any two different unordered edges differ by at least one. Counting the distances shows that an n -point distance-separated set has diameter at least $\binom{n}{2} \approx n^2/2$, and Erdős asked whether the diameter must in fact be at least $(1 - o(1))n^2$. He showed that the answer is no if the dimension may grow with n . The first version of this paper then gave counterexamples with diameter below $0.74n^2$ in a single fixed dimension.

We give a fixed-dimensional counterexample with sharper explicit parameters: for every integer $n \geq 36354$ there is a distance-separated n -point set in $\mathbb{R}^{81794}$ with diameter below $(147/200)n^2 = 0.735n^2$. The finite conclusion has an accompanying Lean 4 proof, including minimum distance at least one for distinct points and the actual set diameter bound.

As in the first version, this construction replaces each vertex of a large “macro” simplex by a cluster of points. We use a standard Gram-deficit completion to arrange those clusters on circles in mutually orthogonal planes. The new arrangement makes every distance between two clusters an exact, explicit, increasing function of two “digits”, and it reduces the number of coordinates from $9m - 1$ to $3m - 1$ for m clusters. A single quadratic-residue ruler then controls both the distances inside the clusters and the digits between them. The proof is self-contained apart from Bertrand’s postulate.

1. INTRODUCTION

1.1. Separated distances and the counting bound. Let X be a finite set of points in a Euclidean space $\mathbb{R}^d$. An *edge* of X is an unordered pair $\{x, y\}$ of distinct points of X , and its *length* is $\|x - y\|$. We call X *distance-separated* if the lengths of any two different edges differ by at least one:

$$(1.1) \quad \left| \|x - y\| - \|u - v\| \right| \geq 1 \quad \text{whenever } \{x, y\} \neq \{u, v\} \text{ are edges of } X.$$

In particular, the $\binom{|X|}{2}$ edge lengths are pairwise distinct.

How small can the diameter of such a set be? There is a simple lower bound. If $|X| \geq 3$, every edge $\{x, y\}$ has length at least one: pick a third point z ; the edges $\{x, z\}$ and $\{y, z\}$ are different, so by (1.1) and the triangle inequality

$$1 \leq \left| \|x - z\| - \|y - z\| \right| \leq \|x - y\|.$$

Hence the sorted edge lengths $\ell_1 < \ell_2 < \dots < \ell_N$, where $N = \binom{|X|}{2}$, satisfy $\ell_1 \geq 1$ and $\ell_{t+1} \geq \ell_t + 1$, so $\ell_t \geq t$ for every t . Taking $t = N$ gives the *counting bound*

$$(1.2) \quad \text{diam } X \geq \binom{|X|}{2} = \left(\frac{1}{2} - o(1) \right) |X|^2.$$

On the real line the truth is twice as large: an n -point distance-separated subset of $\mathbb{R}$ has diameter at least $n^2 - 3n^{3/2}$ (Proposition 7.1 below). Erdős asked whether the same holds in every dimension, that is, whether $\text{diam } X \geq (1 - o(1))n^2$ for every distance-separated n -point set X in any Euclidean space; see Erdős [1, Problem 20]. This is Erdős Problem 670.

Ho [3] showed that the answer is negative if the ambient dimension may grow with n : for infinitely many n there are distance-separated n -point sets in $\mathbb{R}^{n^2-n}$ of diameter $(1 - 1/\pi^2 + o(1))n^2$. Ho also gave the stronger proved asymptotic coefficient $(\pi + \sqrt{\pi^2 - 4})/(2\pi) = 0.885589\dots$ for his high-dimensional construction [3, Remark 10]. He pointed out that this leaves the question in a *fixed* dimension open [3, Remark 9]. The first version of this paper [4] constructed distance-separated n -point sets in $\mathbb{R}^{458999}$ with diameter below $0.74n^2$ for every $n \geq 68000$.

To state results in fixed dimension, define for $d \geq 1$ and $n \geq 3$

$$\Delta_d(n) = \inf\{\text{diam } X : X \subset \mathbb{R}^d, |X| = n, X \text{ is distance-separated}\}.$$

The infimum is over a nonempty class: for instance $\{1, 2, 4, \dots, 2^{n-1}\} \subset \mathbb{R}$ is distance-separated, since its differences $2^b - 2^a$ are distinct integers. Padding with zero coordinates embeds $\mathbb{R}^d$ in $\mathbb{R}^{d+1}$, so $\Delta_d(n)$ is nonincreasing in d . The counting bound gives $\Delta_d(n) \geq \binom{n}{2}$ for every d . The fixed-dimensional question asks whether, for every fixed d ,

$$\liminf_{n \rightarrow \infty} \frac{\Delta_d(n)}{n^2} \geq 1,$$

equivalently whether $\Delta_d(n) \geq (1 - o(1))n^2$ as $n \rightarrow \infty$. That first construction disproved this in one fixed dimension; the theorem below gives a smaller explicit dimension and coefficient for all sufficiently large n .

1.2. Results. The finite result is an explicit improvement in both ambient dimension and diameter coefficient over the first version of this paper.

Theorem 1.1 (A fixed-dimensional counterexample). *For every integer $n \geq 36354$ there is a distance-separated set $X \subset \mathbb{R}^{81794}$ with $|X| = n$ and*

$$\text{diam } X < \frac{147}{200} n^2 = 0.735 n^2.$$

1.3. The idea: a two-digit counter. Here is the construction in outline; Figures 1 and 2 illustrate it. We build a set of $n = mk$ points, arranged in m clusters of k points each. The number m of clusters is fixed (it determines the dimension, $3m - 1$), while the cluster size k grows with n .

The macro skeleton. Start with the $M = \binom{m}{2}$ consecutive target lengths

$$S(K + 1), S(K + 2), \dots, S(K + M).$$

Here K is a large offset. The edges are numbered $1, \dots, M$ in *colexicographic* order (Figure 5). As in the first version [4], a Gram estimate realizes the required macro vertices q_A in $\mathbb{R}^{m-1}$. Their actual distances are shortened to $\|q_A - q_B\| = \sqrt{D_{AB}^2 - 2\rho^2}$, where $D_{AB} = K + \ell_{AB}$ and $\rho = R/S$. This shortening offsets the radius R of the circles and leaves the displayed consecutive values as the cross-edge baselines.

Clusters. Replace each macro vertex Sq_A by a cluster of k points $x_{A0}, \dots, x_{A,k-1}$ lying on a small circle near Sq_A . The set now has two kinds of edges: *local* edges, inside one cluster, whose lengths are comparatively short; and *cross* edges, between two clusters $A < B$, whose lengths are close to SD_{AB} , where $D_{AB} = K + (\text{label of the macro edge } AB)$.

Cross lengths as a two-digit number. The positions on the circles are chosen so that, for $A < B$,

$$(1.3) \quad \|x_{Ai} - x_{Bj}\| \approx SD_{AB} + s^2 k f_{Ai} + s f_{Bj},$$

where $s > 1$ is a number slightly larger than one and the *digits* $f_{A0} < f_{A1} < \dots < f_{A,k-1}$ are real numbers that increase in steps of about one and span an interval of length less than k . Read (1.3) as a two-digit counter (Figure 2). Increasing the *fine digit* j by one increases the length by about s , slightly more than one. Increasing the *coarse digit* i by one increases it by about $s^2 k$, which is more than the whole range, about sk , of the fine digit. So the k^2 cross lengths between A and B are separated and fill a *block* of width about $s^2 k^2$ around SD_{AB} . Consecutive blocks are S apart,

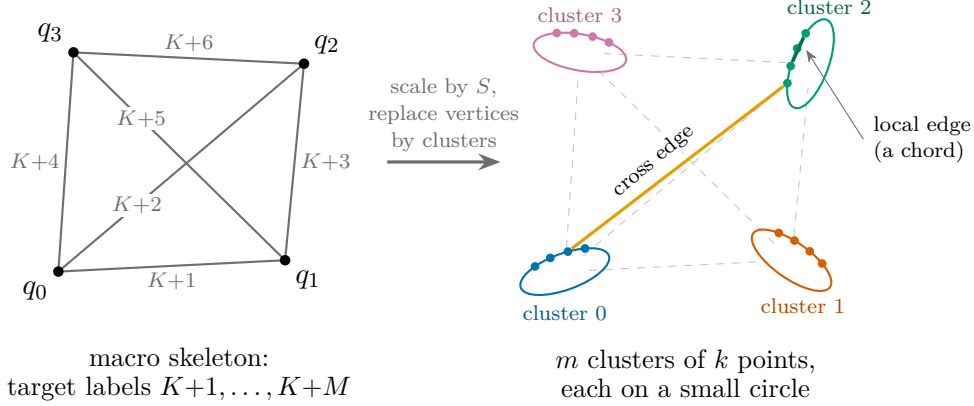


FIGURE 1. A schematic picture with $m = 4$ clusters of $k = 4$ points; it is not to scale. Left: the labels $D_{AB} = K + 1, \dots, K + \binom{m}{2}$ occur in colexicographic order (Figure 5). The actual macro distances are $\sqrt{D_{AB}^2 - 2(R/S)^2}$, before scaling by S . Right: each scaled macro vertex is replaced by k points on a circle of radius R . The circles lie in mutually orthogonal planes, which is not visible in this planar drawing. The radius is small compared with the macro-edge lengths SK , although R/S is large for the chosen parameters.

and the choice $S = s^3 k^2$ leaves room between them. Finally, the local lengths lie far below all cross lengths and are separated by a separate argument.

The diameter coefficient. The largest cross length is about

$$S(K + M) \approx s^3 k^2 \left(K + \frac{m^2}{2} \right) = s^3 \left(\frac{1}{2} + \frac{K}{m^2} \right) (mk)^2.$$

For the finite theorem we take $s = 9/8$, $m \geq 18177$, and $K = \lceil m(m-1)/64 \rceil$. The resulting leading coefficient is $s^3(1/2 + 1/64) = 24057/32768 < 147/200$; the explicit finite margin absorbs the lower-order terms (Section 6).

The difficulty, and how orthogonal circles remove it. Write the points as $x_{Ai} = Sq_A + \eta_{Ai}$ with small perturbations η_{Ai} . Then

$$\|x_{Ai} - x_{Bj}\|^2 = S^2 \|q_A - q_B\|^2 + 2S \langle q_A - q_B, \eta_{Ai} - \eta_{Bj} \rangle + \|\eta_{Ai} - \eta_{Bj}\|^2.$$

The middle term is linear in the perturbations and can produce the two digits. The last term, however, contains the interaction $-2\langle \eta_{Ai}, \eta_{Bj} \rangle$, which depends on i and j jointly and spoils the digit structure. We remove it completely: we put all the points of cluster A on a circle of a common radius R , in a plane orthogonal to the planes of all other clusters. Then $\|\eta_{Ai} - \eta_{Bj}\|^2 = 2R^2$ is a constant, which we absorb by slightly shortening the macro distances. Lemma 2.1 shows that these mutually orthogonal circles cost only $2m$ extra coordinates, while allowing the prescribed macro-space tilts when their complete direction matrix has operator norm at most R , which is what creates the digits. The result is the *exact* formula (Section 5)

$$(1.4) \quad \|x_{Ai} - x_{Bj}\| = \sqrt{\nu^2 + 2\nu T}, \quad \nu = SD_{AB}, \quad T = s^2 k f_{Ai} + s f_{Bj}.$$

This is not linear in T , and its deviation from $\nu + T$ is not bounded as $k \rightarrow \infty$. But it is a fixed increasing function of T , with derivative close to one, and that is all the counter needs (Remark 5.2).

Finally, the local lengths are chords of the circles, determined by differences of the angles. We choose the angles from a quadratic-residue ruler in the spirit of Erdős and Turán [2], all of whose differences are distinct integers. The same ruler, read through a sine, also supplies the digits f_{Ai} . So one ruler serves both purposes.

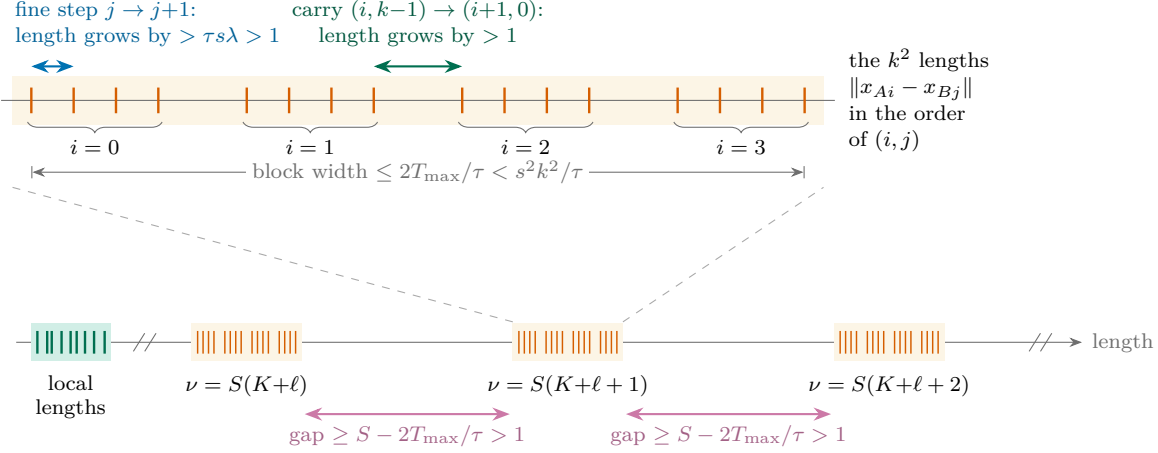


FIGURE 2. Cross lengths form a two-digit counter (schematic, $k = 4$). Bottom: each macro edge AB , with label $\ell = \ell_{AB}$, contributes a block of k^2 cross lengths around $\nu = S(K + \ell)$; consecutive blocks are $S = s^3 k^2$ apart and do not overlap. All local lengths lie below the first block. Top: inside one block the lengths, listed in the lexicographic order of (i, j) , increase by more than one at every step, both at a *fine step* (the fine digit j increases) and at a *carry* (the coarse digit i increases and j resets to 0).

1.4. Changes from the first version. This revision retains the first version’s macro skeleton [4]: the colexicographic labelling, the positive-definiteness estimates for its Gram matrix, and the operator-norm bounds for the two families of “incidence” vectors F_A, G_A attached to it (Lemma 3.1). We reproduce the proofs in Section A so that the paper can be read independently. It also retains the clustered quadratic-residue ruler, with its principal spacing made a free parameter.

What changes is the cluster geometry. Orthogonal-circle arrangements have classical precedents in Lenz’s construction, as reported by Erdős [9]; the use of one tilted circle per macro vertex to encode both local chords and cross digits is the present organization. The first version’s clusters use a separate ruler circle, a quadratic correction, higher harmonics and an extra axis, for a total of $9m - 1$ coordinates. A single circle per cluster, placed by Lemma 2.1, does the work of all of these and needs $3m - 1$ coordinates. The second observation is that one does not need a uniformly bounded additive error in a linear approximation to a cross length; a two-sided bound on its *derivative* suffices (Remark 5.2). This permits the explicit parameters below to satisfy the five separation and geometry conditions with strict margins.

1.5. Organization and notation. Figure 3 shows how the pieces fit together. Section 2 proves the orthogonal-circle completion and computes the cross distances it produces. Section 3 states the macro input. Section 4 constructs the ruler and the digits. Section 5 assembles everything into a finite criterion, Theorem 5.1: five inequalities between a handful of parameters which, if they hold, give a distance-separated set of mk points in $\mathbb{R}^{3m-1}$ for every $k \geq 2$. Section 6 chooses the parameters and proves Theorem 1.1. Section 7 explains what the method does not give, and proves the lower bound on the line. Section A proves the macro input.

Notation. Norms $\|\cdot\|$ and inner products $\langle \cdot, \cdot \rangle$ are Euclidean; $\|\cdot\|_{\text{op}}$ is the operator norm of a matrix. We write $e_0, \dots, e_{m-1}$ for the standard basis of $\mathbb{R}^m$, indexed from zero. Given vectors $V_0, \dots, V_{m-1} \in \mathbb{R}^r$, we also write V for the $r \times m$ matrix with columns $V_A = Ve_A$. For symmetric matrices, $P \succeq Q$ means that $P - Q$ is positive semidefinite, and $P[x] = x^\top P x$ is the associated quadratic form. $\mathbf{1}_{\mathcal{P}}$ equals 1 if the statement $\mathcal{P}$ is true and 0 otherwise. Capital letters A, B, J

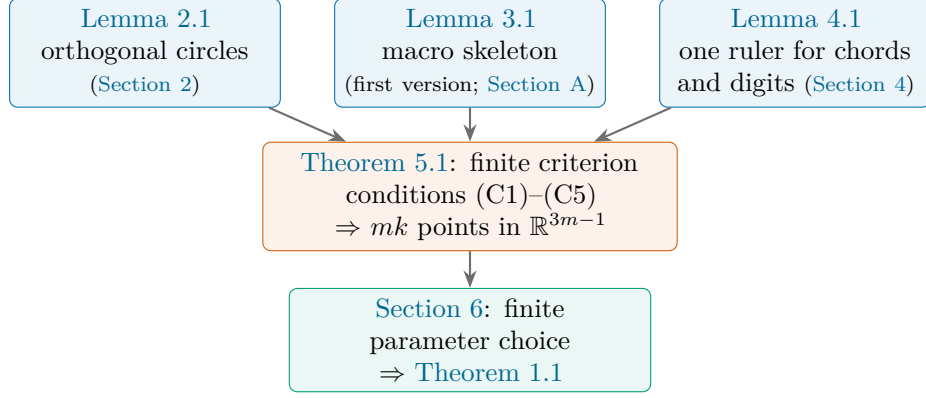


FIGURE 3. Logical structure of the paper.

index clusters ($0 \leq A < m$) and lower-case i, j index points within a cluster ($0 \leq i < k$). Finally, $H_m = \sum_{j=1}^m 1/j$ is the m -th harmonic number.

2. THE GEOMETRIC PRINCIPLE: ORTHOGONAL CIRCLES

We want to place one circle of radius R around each macro vertex. Each circle must tilt into the macro space in a prescribed direction U_A , because the inner products of U_A with the macro edges will produce the digits. At the same time the circles should lie in mutually orthogonal planes, so that they do not interact. The following lemma shows that both requirements can be met with $2m$ extra coordinates, provided the whole matrix of directions has operator norm at most R . The Gram-deficit square root is the standard defect-operator completion for a contraction after rescaling [8]. The quantitative input here is the bound on the complete direction matrix U .

Lemma 2.1 (Orthogonal-circle completion). *Let $R > 0$, and let U be a real $r \times m$ matrix with columns $U_0, \dots, U_{m-1} \in \mathbb{R}^r$ and $\|U\|_{\text{op}} \leq R$. Put*

$$W = (R^2 I_m - U^\top U)^{1/2},$$

the positive semidefinite square root. For $0 \leq A < m$ and $z \in \mathbb{R}$ define

$$(2.1) \quad \eta_A(z) = (U_A \sin z, W e_A \sin z, R e_A \cos z) \in \mathbb{R}^r \oplus \mathbb{R}^m \oplus \mathbb{R}^m.$$

Then for all $z, w \in \mathbb{R}$,

$$(2.2) \quad \|\eta_A(z)\| = R,$$

$$(2.3) \quad \langle \eta_A(z), \eta_B(w) \rangle = 0 \quad (A \neq B),$$

$$(2.4) \quad \|\eta_A(z) - \eta_A(w)\| = 2R \left| \sin \frac{z-w}{2} \right|.$$

In words: η_A traces a circle of radius R centred at the origin, and the m circle planes are mutually orthogonal. Only $r + 2m$ coordinates are used, however many points are later placed on each circle.

Proof. The matrix $R^2 I_m - U^\top U$ is positive semidefinite because $\|U\|_{\text{op}} \leq R$, so W exists, and $U^\top U + W^\top W = R^2 I_m$. Put

$$a_A = (U_A, W e_A, 0), \quad b_A = (0, 0, R e_A).$$

Then $\langle a_A, a_B \rangle = (U^\top U + W^\top W)_{AB} = R^2 \mathbf{1}_{A=B}$ and $\langle b_A, b_B \rangle = R^2 \mathbf{1}_{A=B}$, while $\langle a_A, b_B \rangle = 0$ for all A, B . Thus the $2m$ vectors a_A, b_A are pairwise orthogonal and all have norm R . Since $\eta_A(z) = a_A \sin z + b_A \cos z$, the curve η_A is a circle of radius R in the plane spanned by a_A and b_A , and these planes are mutually orthogonal. The identities (2.2)–(2.4) follow at once; for the last one, $\|\eta_A(z) - \eta_A(w)\|^2 = 2R^2 - 2R^2 \cos(z-w) = 4R^2 \sin^2 \frac{z-w}{2}$. $\square$

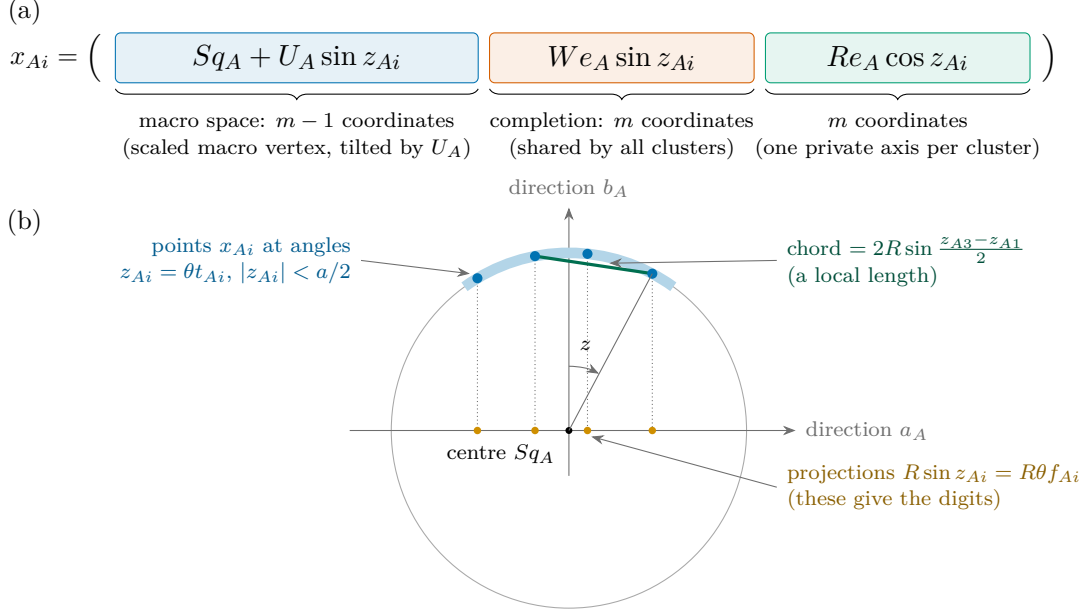


FIGURE 4. (a) The $3m - 1$ coordinates of a point. The first block carries the scaled macro vertex and the tilt U_A ; the other two blocks complete the circles so that they become mutually orthogonal. Indeed, the $2m$ vectors $a_A = (U_A, We_A, 0)$ and $b_A = (0, 0, Re_A)$ are pairwise orthogonal and have length R , and $x_{Ai} = (Sq_A, 0, 0) + a_A \sin z_{Ai} + b_A \cos z_{Ai}$. (b) The circle of cluster A , in the plane of a_A and b_A (angles exaggerated). The points use only a short arc, of angular width at most $a \leq 1$. Two quantities are read off the same angles z_{Ai} : chords, which are the local lengths, and projections onto the tilted direction a_A , which produce the digits of the cross lengths.

Cross distances. Now choose macro vertices $q_0, \dots, q_{m-1} \in \mathbb{R}^r$ and a scale $S > 0$, and consider points of the form

$$(2.5) \quad x_{Ai} = (Sq_A, 0, 0) + \eta_A(z_{Ai}).$$

For $A \neq B$, expanding $\|x_{Ai} - x_{Bj}\|^2$ and using (2.2)–(2.3) gives the exact identity

$$(2.6) \quad \|x_{Ai} - x_{Bj}\|^2 = \underbrace{S^2 \|q_A - q_B\|^2 + 2R^2}_{\text{depends only on } A, B} + 2S \langle q_A - q_B, U_A \sin z_{Ai} - U_B \sin z_{Bj} \rangle.$$

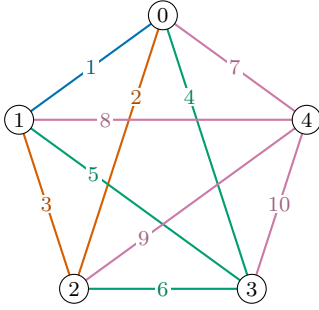
The first two terms can be prescribed together: if the macro vertices are chosen with squared distances *shortened* by $2(R/S)^2$, then these two terms add up to the desired squared macro length. What remains is a term *linear* in $\sin z_{Ai}$ and $\sin z_{Bj}$, with no interaction between them. No quadratic or second-harmonic correction is needed.

3. THE MACRO SKELETON

The macro edges AB , $0 \leq A < B < m$, are labelled in *colexicographic order*: first by the larger endpoint B , then by the smaller endpoint A . Explicitly,

$$(3.1) \quad \ell_{AB} = \binom{B}{2} + A + 1, \quad D_{AB} = K + \ell_{AB} \quad (0 \leq A < B < m),$$

and we put $D_{BA} = D_{AB}$. The labels ℓ_{AB} run through $1, 2, \dots, M$ exactly once, where $M = \binom{m}{2}$ (Figure 5). The number $K > 0$ is an offset, and D_{AB} is the length that the macro edge AB will have, in units of S .



$A \setminus B$	1	2	3	4
0	1	2	4	7
1		3	5	8
2			6	9
3				10

$\ell_{AB} = \binom{B}{2} + A + 1$:
read the table
column by column

FIGURE 5. Colexicographic labels for $m = 5$. The edges are listed by increasing larger endpoint B (one colour for each B), and then by increasing smaller endpoint A . The target cross-edge baseline is $D_{AB} = K + \ell_{AB}$; the realized macro distance is $\sqrt{D_{AB}^2 - 2\rho^2}$, where $\rho = R/S$. The target labels are $K + 1, \dots, K + \binom{m}{2}$.

The following lemma is the macro input. It says that the colex lengths, shortened as required by (2.6), are realized by an honest simplex, and it controls two families of vectors attached to it.

Lemma 3.1 (Macro skeleton from the first version). *Let $m \geq 4$, $K > 0$ and $\rho \geq 0$ satisfy*

$$(3.2) \quad K \geq m, \quad K \geq 16384H_m^2, \quad \rho \leq K/4.$$

(i) *There are affinely independent points $q_0, \dots, q_{m-1} \in \mathbb{R}^{m-1}$ with*

$$(3.3) \quad \|q_A - q_B\|^2 = D_{AB}^2 - 2\rho^2 \quad (A \neq B).$$

(ii) *For each A there are unique vectors $F_A, G_A \in \mathbb{R}^{m-1}$ such that, for every $J \neq A$,*

$$(3.4) \quad \langle q_A - q_J, F_A \rangle = D_{AJ} \mathbf{1}_{J < A}, \quad \langle q_A - q_J, G_A \rangle = D_{AJ} \mathbf{1}_{J > A}.$$

(iii) *The $(m-1) \times m$ matrices F and G with these columns satisfy*

$$(3.5) \quad \|F\|_{\text{op}} \leq 24\sqrt{K+m}, \quad \|G\|_{\text{op}} \leq 60\sqrt{K+m}.$$

This is the first version's macro input [4, Lemmas 2–3]; a complete proof in the present notation is given in Section A. Part (ii) is immediate from (i): the $m-1$ vectors $q_A - q_J$ ($J \neq A$) form a basis of $\mathbb{R}^{m-1}$. The substance is part (iii). Note that it bounds the *whole* matrices F and G , not just their individual columns. This is essential, because Lemma 2.1 needs a bound on the operator norm of the whole matrix U .

The vector F_A “sees” only the macro edges from A down to smaller vertices, and G_A only those from A up to larger vertices. In a cross edge between clusters $A < B$, we shall let the smaller endpoint carry the coarse digit and the larger one the fine digit. Accordingly, given $s > 1$, a cluster size k and an angular scale $\theta > 0$, we set

$$(3.6) \quad U_A = \frac{s}{\theta}(F_A + sk G_A) \quad (0 \leq A < m).$$

Then for $A < B$ the definitions (3.4) give the two projections

$$(3.7) \quad \langle q_A - q_B, U_A \rangle = \frac{s^2 k}{\theta} D_{AB} \quad (\text{coarse}), \quad \langle q_B - q_A, U_B \rangle = \frac{s}{\theta} D_{AB} \quad (\text{fine}).$$

Since $sk \geq 1$, the bounds (3.5) give

$$(3.8) \quad \|U\|_{\text{op}} \leq \frac{s}{\theta}(24 + 60sk)\sqrt{K+m} \leq \frac{84s^2 k \sqrt{K+m}}{\theta}.$$

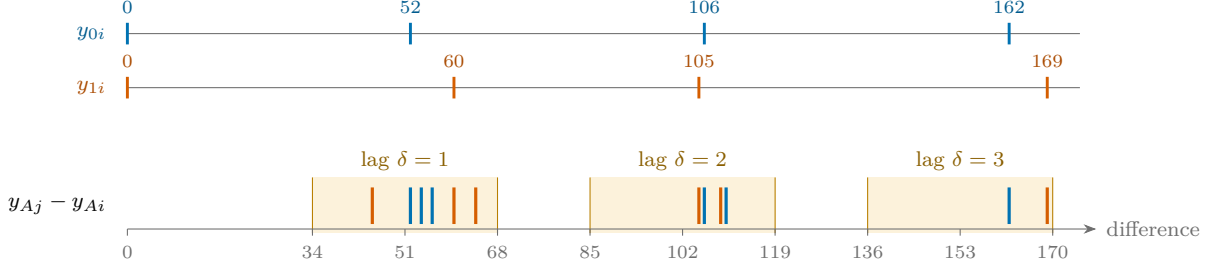


FIGURE 6. The ruler of Lemma 4.1 for $m = 2$ clusters of $k = 4$ points, with $L = 3$ and $p = 17$. Top: the marks y_{0i} (blue) and y_{1i} (red). Bottom: all $2\binom{4}{2} = 12$ differences $y_{Aj} - y_{Ai}$. A difference with lag $\delta = j - i$ lies in the shaded window from $(L\delta - 1)p$ to $(L\delta + 1)p$. Inside a window, the quadratic residues keep all differences apart, even across the two clusters.

4. ONE RULER FOR LOCAL LENGTHS AND DIGITS

The angles on the circles come from the following ruler. It is a quadratic-residue construction of Erdős–Turán type [2], with a linear term depending on the cluster as in the first version [4]. For an integer u we write $[u]_p$ for the least nonnegative residue of u modulo p .

Lemma 4.1 (Clustered ruler). *Let $m, k \geq 2$ and $L \geq 3$ be integers, and let p be a prime with $2mk < p < 4mk$. Define the integers*

$$(4.1) \quad y_{Ai} = Lpi + [i^2 + 2kAi]_p \quad (0 \leq A < m, 0 \leq i < k).$$

Then the differences $y_{Aj} - y_{Ai}$, taken over all clusters A and all $0 \leq i < j < k$, are positive and pairwise distinct. Moreover, with

$$(4.2) \quad \kappa = 1 - \frac{1}{L}, \quad h = \frac{k - \kappa}{2}, \quad t_{Ai} = \frac{y_{Ai}}{Lp} - h,$$

the normalized positions t_{Ai} satisfy

$$(4.3) \quad |t_{Ai}| \leq h < \frac{k}{2}, \quad t_{A,i+1} - t_{Ai} > \kappa, \quad t_{A,k-1} - t_{A0} < k - \kappa.$$

So each row $t_{A0} < \dots < t_{A,k-1}$ is an almost evenly spaced sequence, with steps between $\kappa = 1 - 1/L$ and $1 + 1/L$, inside $[-h, h]$; but all the differences of the underlying integers, across all clusters, are distinct (Figure 6). Taking L large makes the spacing nearly uniform.

Proof. Fix a lag $1 \leq \delta < k$ and write $g_{Ai\delta} = y_{A,i+\delta} - y_{Ai}$ for $0 \leq i < k - \delta$. The residue parts of $y_{A,i+\delta}$ and y_{Ai} lie in $[0, p)$, and $(i + \delta)^2 + 2kA(i + \delta) - i^2 - 2kAi = \delta(2i + \delta + 2kA)$, so

$$(4.4) \quad (L\delta - 1)p < g_{Ai\delta} < (L\delta + 1)p, \quad g_{Ai\delta} \equiv \delta(2i + \delta + 2kA) \pmod{p}.$$

In particular every difference is positive. Differences with different lags lie in disjoint windows, since $L \geq 2$. For a fixed lag, the integers $2i + \delta + 2kA$ lie in $[1, 2mk) \subset [1, p)$, and they are pairwise distinct: $2i + \delta + 2kA = 2i' + \delta + 2kA'$ forces $i - i' = k(A' - A)$, and as $|i - i'| < k$ this gives $A = A'$ and $i = i'$. Since $0 < \delta < p$, multiplication by δ is injective modulo p , so the residues of the $g_{Ai\delta}$ are pairwise distinct as well. This proves that all differences are distinct.

For the bounds, $0 \leq y_{Ai} \leq Lp(k - 1) + p - 1$, so $0 \leq y_{Ai}/(Lp) < k - 1 + 1/L = k - \kappa = 2h$; this gives $|t_{Ai}| \leq h$. The consecutive differences satisfy $g_{Ai1}/(Lp) > (L - 1)/L = \kappa$ by (4.4), and the total range is less than $2h = k - \kappa$. $\square$

By Bertrand's postulate (for every integer $N \geq 2$ there is a prime p with $N < p < 2N$), a prime as in Lemma 4.1 exists. We now turn the positions t_{Ai} into angles and digits. Fix $0 < a \leq 1$, which

TABLE 1. The parameters of [Theorem 5.1](#) and the finite choice used to prove [Theorem 1.1](#) in [Section 6](#).

	role	finite choice
m	number of clusters; dimension $3m - 1$	$18177 \leq m \leq 27265$
k	points per cluster	any $k \geq 2$
K	offset of the macro lengths $D_{AB} = K + \ell_{AB}$	$\lceil m(m-1)/64 \rceil$
s	slack factor, $s > 1$; scale $S = s^3 k^2$	$9/8$
a	angular width of each cluster; $\theta = a/k$	$49/100$
L	spacing factor of the ruler	12
C	radius constant; radius $R = Cmk^2$	101
derived: $\kappa = 1 - 1/L$, $\gamma = 1 - a^2/8$, $\lambda = \kappa\gamma$, $M = \binom{m}{2}$, $\rho = R/S = Cm/s^3$		

will be the angular width of every cluster, and put

$$(4.5) \quad \theta = \frac{a}{k}, \quad z_{Ai} = \theta t_{Ai}, \quad f_{Ai} = \frac{\sin z_{Ai}}{\theta} = \frac{\sin(\theta t_{Ai})}{\theta}, \quad \gamma = 1 - \frac{a^2}{8}, \quad \lambda = \kappa\gamma.$$

The angle z_{Ai} places the point x_{Ai} on its circle, and f_{Ai} is its digit. Since $|t_{Ai}| \leq h < k/2$, all angles satisfy $|z_{Ai}| < a/2 \leq 1/2$. On this range the function $t \mapsto \sin(\theta t)/\theta$ has derivative $\cos(\theta t) \in [\gamma, 1]$, because $\cos u \geq 1 - u^2/2$. By the mean value theorem, (4.3) becomes

$$(4.6) \quad |f_{Ai}| \leq h, \quad f_{A,i+1} - f_{Ai} > \lambda, \quad f_{A,k-1} - f_{A0} < k - \kappa.$$

So the digits of each cluster increase in steps larger than λ (a number slightly below one) and span an interval shorter than k . Since the angles themselves come from the ruler, there is no separate local geometry to fit into the construction.

5. A FINITE CRITERION

We now assemble the construction. All the numerical requirements are collected into five inequalities, (C1)–(C5), on six inputs m, L, s, a, C, K , summarized in [Table 1](#). The tolerance τ is determined by these inputs. Since k occurs in none of the inequalities, one feasible choice works for every cluster size $k \geq 2$.

Theorem 5.1 (Finite criterion). *Let $m \geq 4$ and $L \geq 3$ be integers, and let $s > 1$, $0 < a \leq 1$, $C, K > 0$ be real numbers. With $\kappa, \gamma, \lambda, M$ as in [Table 1](#), define the slope tolerance*

$$(5.1) \quad \tau = \sqrt{1 - \frac{1}{s(K+1)}} \in (0, 1).$$

Suppose that

$$(C1) \quad \tau s \lambda > 1,$$

$$(C2) \quad K \geq \max\{m, 16384H_m^2\},$$

$$(C3) \quad K \geq 4Cm/s^3,$$

$$(C4) \quad Cm \geq \frac{84s^2}{a} \sqrt{K+m},$$

$$(C5) \quad Ca\gamma > 4L.$$

Then for every integer $k \geq 2$ there is a distance-separated set of mk distinct points in $\mathbb{R}^{3m-1}$ with diameter at most

$$(5.2) \quad \left[s^3(K + M) + \frac{s^2}{2\tau} \right] k^2.$$

The definition (5.1) makes the cross-length slope budget an identity. The local-versus-cross guard follows automatically: by (C3), $s^3K \geq 4Cm$. Also (C5), $L \geq 3$, $a \leq 1$ and $\gamma \leq 1$ give $Cm \geq Ca > 12$. Hence $(4 - a)Cm \geq 3Cm > 36 > 1$, and therefore

$$(5.3) \quad s^3K \geq 4Cm > Cam + 1.$$

The conditions have the following roles in the proof:

- (C1): a fine step increases the cross length by more than one;
- (C2), (C3): [Lemma 3.1](#) applies with the shortening $\rho = R/S$ required by (2.6); (C3) also puts cross lengths above local lengths;
- (C4): the radius R is at least $\|U\|_{\text{op}}$, so that [Lemma 2.1](#) applies;
- (C5): chords of the circles grow by more than one per unit of the ruler.

Proof. Fix $k \geq 2$. We construct the points and then compare the lengths of all pairs of edges: local with local, cross with cross, and local with cross.

Step 1: construction. Set

$$(5.4) \quad S = s^3k^2, \quad R = Cmk^2, \quad \rho = \frac{R}{S} = \frac{Cm}{s^3}, \quad \theta = \frac{a}{k}.$$

By (C2) and (C3), [Lemma 3.1](#) applies with this ρ . Take its macro vertices $q_A \in \mathbb{R}^{m-1}$ and the vectors U_A from (3.6). By (3.8) and (C4),

$$\|U\|_{\text{op}} \leq \frac{84s^2k\sqrt{K+m}}{a/k} = \frac{84s^2}{a}\sqrt{K+m}k^2 \leq Cmk^2 = R,$$

so [Lemma 2.1](#) applies with $r = m - 1$. Take the ruler of [Lemma 4.1](#) and the angles $z_{Ai} = \theta t_{Ai}$ of (4.5), and define, as in (2.5),

$$(5.5) \quad x_{Ai} = (Sq_A + U_A \sin z_{Ai}, \quad We_A \sin z_{Ai}, \quad Re_A \cos z_{Ai}) \in \mathbb{R}^{m-1} \oplus \mathbb{R}^m \oplus \mathbb{R}^m,$$

where $W = (R^2I_m - U^\top U)^{1/2}$ ([Figure 4\(a\)](#)). These points lie in $\mathbb{R}^{3m-1}$.

Step 2: local edges. Let A be a cluster and $i < j$. By (2.4), the local length is a chord:

$$(5.6) \quad \|x_{Aj} - x_{Ai}\| = 2R \sin \frac{z_{Aj} - z_{Ai}}{2} = \phi(y_{Aj} - y_{Ai}), \quad \text{where } \phi(g) = 2R \sin \frac{\theta g}{2Lp}.$$

Thus every local length, in every cluster, is the value of one fixed function ϕ at the corresponding ruler difference $g = y_{Aj} - y_{Ai}$, which is a positive integer with $g/(Lp) < k$. For $0 \leq g \leq Lpk$ we have $\theta g/(2Lp) \leq a/2$, so

$$\phi'(g) = \frac{R\theta}{Lp} \cos \frac{\theta g}{2Lp} \geq \frac{R\theta\gamma}{Lp} > \frac{Camk\gamma}{L \cdot 4mk} = \frac{Ca\gamma}{4L} > 1,$$

using $R\theta = Camk$, $p < 4mk$ and (C5). By [Lemma 4.1](#), distinct local edges have distinct integer differences g , even when they lie in different clusters. Hence, by the mean value theorem, any two local lengths differ by more than one. Likewise every local length is at least $\phi(1) > \phi(0) + 1 = 1$. Since $2\sin(u/2) \leq u$, the local lengths are also bounded above:

$$(5.7) \quad \|x_{Aj} - x_{Ai}\| \leq R(z_{Aj} - z_{Ai}) < R\theta k = Camk^2.$$

Step 3: an exact formula for cross lengths. Let $A < B$, and put

$$(5.8) \quad \nu = SD_{AB}, \quad T_{AiBj} = s^2k f_{Ai} + s f_{Bj}.$$

In (2.6), the shortened metric (3.3) with $\rho = R/S$ gives $S^2\|q_A - q_B\|^2 + 2R^2 = S^2D_{AB}^2 = \nu^2$, and the projections (3.7) give

$$2S\langle q_A - q_B, U_A \sin z_{Ai} - U_B \sin z_{Bj} \rangle = 2SD_{AB} \left(\frac{s^2k}{\theta} \sin z_{Ai} + \frac{s}{\theta} \sin z_{Bj} \right) = 2\nu T_{AiBj}.$$

Therefore

$$(5.9) \quad \|x_{Ai} - x_{Bj}\| = \Phi_\nu(T_{AiBj}), \quad \text{where } \Phi_\nu(T) = \sqrt{\nu^2 + 2\nu T}.$$

We now bound the digit sum and the slope of Φ_ν . Note first that (C1) implies $s\kappa \geq s\lambda > 1/\tau > 1$ and $s > 1/\tau$, because $\lambda \leq \kappa \leq 1$. By (4.6), $|T_{AiBj}| \leq T_{\max}$, where

$$(5.10) \quad T_{\max} = s(sk + 1)h = \frac{s(sk + 1)(k - \kappa)}{2}, \quad 2T_{\max} = s^2k^2 - s(s\kappa - 1)k - s\kappa < s^2k^2.$$

Every macro length satisfies $D_{AB} \geq K + 1$, so $\nu \geq \nu_0 = S(K + 1)$. Hence, for $|T| \leq T_{\max}$ and by (5.1),

$$\frac{2|T|}{\nu} < \frac{s^2k^2}{s^3k^2(K + 1)} = \frac{1}{s(K + 1)} \leq 1 - \tau^2.$$

In particular $\nu^2 + 2\nu T > 0$. Since $\Phi'_\nu(T) = (1 + 2T/\nu)^{-1/2}$ and $1 + 2T/\nu \in [\tau^2, 2 - \tau^2]$, we obtain

$$(5.11) \quad \tau \leq \Phi'_\nu(T) \leq \frac{1}{\tau} \quad \text{and} \quad |\Phi_\nu(T) - \nu| \leq \frac{T_{\max}}{\tau} \quad (|T| \leq T_{\max}).$$

For the lower bound on the slope we used $2 - \tau^2 \leq \tau^{-2}$, which is equivalent to $(1 - \tau^2)^2 \geq 0$; the second bound follows from the first since $\Phi_\nu(0) = \nu$.

Step 4: cross lengths are separated. List the cross edges as in Figure 2: first by the label ℓ_{AB} of the macro edge, and within each macro edge by (i, j) in lexicographic order. We show that each length in this list exceeds the previous one by more than one. Three kinds of steps occur.

Fine step: $(i, j) \rightarrow (i, j + 1)$. By (4.6), T increases by $s(f_{B,j+1} - f_{Bj}) > s\lambda$. Since ν is unchanged, (5.11) shows that the length increases by more than $\tau s\lambda > 1$, by (C1).

Carry: $(i, k - 1) \rightarrow (i + 1, 0)$. By (4.6), T increases by

$$s^2k(f_{A,i+1} - f_{Ai}) - s(f_{B,k-1} - f_{B0}) > s^2k\lambda - s(k - \kappa) = s[(s\lambda - 1)k + \kappa] \geq s\kappa.$$

So the length increases by more than $\tau s\kappa \geq \tau s\lambda > 1$.

Macro step: from the last pair of the macro edge with label ℓ to the first pair of the macro edge with label $\ell + 1$. Here ν increases by exactly S . By (5.11), all lengths of one macro edge lie within $T_{\max}/\tau$ of its ν , so the length increases by at least $S - 2T_{\max}/\tau$. Using (5.10),

$$(5.12) \quad S - \frac{2T_{\max}}{\tau} = s^2 \left(s - \frac{1}{\tau} \right) k^2 + \frac{s(s\kappa - 1)}{\tau} k + \frac{s\kappa}{\tau} > 1,$$

since all three terms are positive and the last one exceeds one.

Consecutive cross lengths in the list therefore differ by more than one, and so do any two cross lengths.

Step 5: local versus cross lengths, and the diameter. By (5.11), (5.10) and $s > 1/\tau$, every cross length is at least

$$\nu_0 - \frac{T_{\max}}{\tau} > s^3(K + 1)k^2 - \frac{s^2k^2}{2\tau} = s^3Kk^2 + s^2 \left(s - \frac{1}{2\tau} \right) k^2 > s^3Kk^2 \geq (Cam + 1)k^2,$$

the last step by (5.3). By (5.7), this exceeds every local length by more than $k^2 > 1$. Together with Steps 2 and 4, this proves that the set is distance-separated; as all lengths are positive, its mk points are distinct. Finally, the largest macro length is $D_{AB} = K + M$, and the cross lengths dominate the local ones, so by (5.11) and (5.10)

$$\text{diam}\{x_{Ai}\} \leq S(K + M) + \frac{T_{\max}}{\tau} \leq \left[s^3(K + M) + \frac{s^2}{2\tau} \right] k^2. \quad \square$$

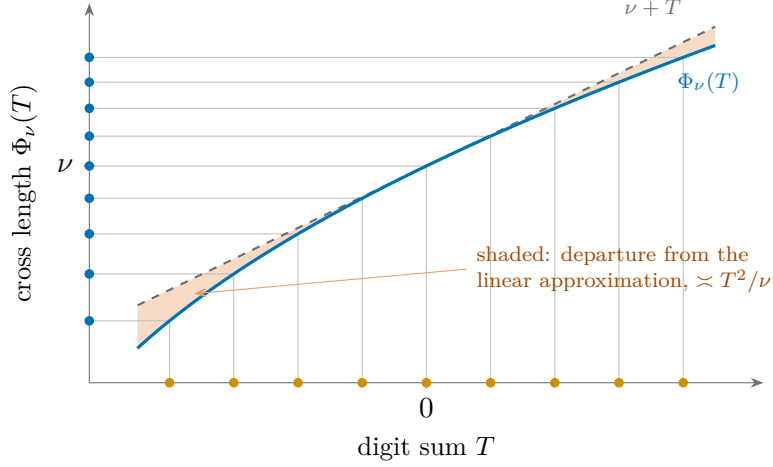


FIGURE 7. The cross length $\Phi_\nu(T) = \sqrt{\nu^2 + 2\nu T}$ as a function of the digit sum T , with the range of T/ν greatly exaggerated (in the construction, $|T|/\nu < 1/(2s(K+1))$). The curve departs from the line $\nu + T$ (shaded) by an amount that grows without bound as $k \rightarrow \infty$. This does not matter: the proof only uses that Φ_ν is increasing with slope in $[\tau, 1/\tau]$. Equally spaced digit sums (orange) are therefore sent to lengths (blue) whose spacings change by a factor of at most $1/\tau$, so separated digit sums give separated lengths.

Remark 5.2 (A derivative bound replaces an additive approximation). Expanding (5.9) gives $\Phi_\nu(T) = \nu + T + O(T^2/\nu)$. Here T is of order k^2 and so is ν (for fixed m), so the error term is of order k^2 and is *not* bounded as $k \rightarrow \infty$; a linear approximation to the cross lengths would therefore be useless. The proof never uses one. Within one macro edge it compares values of the same increasing function Φ_ν , and only the slope bounds (5.11) matter (Figure 7). Between different macro edges, a gap of order k^2 is available. This is what removes the quadratic correction terms of the original construction.

6. A CONCRETE CHOICE OF PARAMETERS

We verify Theorem 5.1 for every $m \geq 18177$ with

$$(6.1) \quad s = \frac{9}{8}, \quad a = \frac{49}{100}, \quad L = 12, \quad C = 101, \quad K = \left\lceil \frac{m(m-1)}{64} \right\rceil.$$

These simple rational values reduce the radius budget while retaining strict margins in every condition. They give $\kappa = 11/12$, $\gamma = 77599/80000$ and $\lambda = 853589/960000$.

Preliminary bounds. Grouping the terms of H_{18177} into the dyadic blocks $[2^t, 2^{t+1})$, each of which contributes at most one, gives $H_{18177} \leq 16 < 18177/1100$. Since $H_{m+1} = H_m + 1/(m+1)$ and $1/(m+1) \leq 1/1100$, induction on m gives

$$H_m \leq \frac{m}{1100} \quad (m \geq 18177).$$

From $m(m-1)/64 \leq K < m(m-1)/64 + 1$ we also get

$$(6.2) \quad K \geq 284m, \quad K + m \leq \frac{m^2}{63}, \quad K \geq \frac{m(m-1)}{64} \geq 16384 \left(\frac{m}{1100} \right)^2.$$

The first holds since $m-1 \geq 18176 = 64 \cdot 284$. The second reduces to $m^2 \geq 3969m + 4032$, and the third to $(m-1)/m \geq 64 \cdot 16384/1100^2$; both follow at $m = 18177$ and remain true as m increases.

For a convenient rational lower bound on the derived tolerance, put $\tau_* = 9999/10000$. By $K \geq 284m$ and $m \geq 18177$,

$$\frac{1}{s(K+1)} \leq \frac{8}{46460421} < \frac{19999}{100000000} = 1 - \tau_*^2, \quad \text{so } \tau > \tau_*.$$

The five conditions.

$$(C1) \quad \tau s \lambda > \tau_* s \lambda = 1 + \frac{5109233}{25600000000} > 1.$$

$$(C2) \quad K \geq 284m \geq m, \text{ and } K \geq 16384(m/1100)^2 \geq 16384H_m^2 \text{ by (6.2).}$$

$$(C3) \quad 4C/s^3 = 206848/729 = 284 - 188/729 < 284, \text{ so } K \geq 284m > 4Cm/s^3.$$

$$(C4) \quad \text{By (6.2), } \frac{84s^2}{a} \sqrt{K+m} \leq \frac{84s^2}{a\sqrt{63}} m < 28m < 101m = Cm.$$

$$(C5) \quad \frac{Ca\gamma}{4L} = 1 + \frac{37451}{384000000} > 1.$$

The diameter. Put $c_* = s^3(33/64) = 24057/32768$. Since $K < M/32 + 1$ and $M = m(m-1)/2$, the bound (5.2) gives, for all $m \geq 18177$ and $k \geq 2$, a distance-separated set X of mk points in $\mathbb{R}^{3m-1}$ with

$$(6.3) \quad \text{diam } X < [c_*m(m-1) + s^3 + s^2/(2\tau_*)]k^2 < c_*(mk)^2.$$

The last comparison holds already for $m \geq 4$, since $4c_* - (s^3 + s^2/(2\tau_*)) = 8008623/9101312 > 0$. This keeps the leading coefficient visible instead of replacing it by the looser $147/200$ finite-set cap.

Proof of Theorem 1.1. Given $n \geq 36354$, put

$$k = \left\lfloor \frac{n}{18177} \right\rfloor, \quad m = \left\lceil \frac{n}{k} \right\rceil.$$

Writing $n = 18177k + b$ with $0 \leq b < 18177$, we have $k \geq 2$ and $m = 18177 + \lceil b/k \rceil$, and hence

$$18177 \leq m \leq 18177 + \lceil 18176/2 \rceil = 27265, \quad n \leq mk < n + k \leq \left(1 + \frac{1}{18177}\right)n.$$

Take the mk -point set given by (6.3), keep any n of its points, and pad with zero coordinates up to dimension $3 \cdot 27265 - 1 = 81794$. Passing to a subset preserves (1.1) and cannot increase the diameter. Therefore

$$\text{diam } X < c_* \left(\frac{18178}{18177} \right)^2 n^2 = \frac{220816318833}{300740452352} n^2 < \frac{147}{200} n^2. \quad \square$$

7. WHAT THE METHOD DOES NOT GIVE

The completion lemma holds in every Euclidean space, but using it has a dimension cost: it consumes m mutually orthogonal circle planes, in addition to at most $m-1$ macro directions. The explicit theorem uses $m \leq 27265$, so this mechanism does not produce a counterexample in a prescribed low dimension.

In fact, within this construction the dependence on m cannot be removed by a change of coordinates. If each cluster has at least three points, the differences of points in cluster A span the plane of its circle (three distinct points of a circle are never collinear). These m planes are mutually orthogonal, so the affine span of the whole configuration has dimension at least $2m$. This is a limitation of the present mechanism, not an impossibility theorem for other constructions.

There is, however, a genuine obstruction in one dimension: there, the coefficient 1 conjectured by Erdős is correct. The following short proof does not require the points to be integers.

Proposition 7.1 (The line). *Every distance-separated set $X \subset \mathbb{R}$ with $|X| = n \geq 4$ satisfies*

$$\text{diam } X \geq n^2 - 3n^{3/2}.$$

In particular $\liminf_{n \rightarrow \infty} \Delta_1(n)/n^2 \geq 1$.

Proof. Write $X = \{x_1 < \dots < x_n\}$, let $D = x_n - x_1$, and put $w = \lfloor \sqrt{n} \rfloor$. Consider the *short* lengths $x_{i+j} - x_i$ with $1 \leq j \leq w$ and $1 \leq i \leq n - j$. There are

$$Q = \sum_{j=1}^w (n - j) = wn - \frac{w(w+1)}{2}$$

of them. They are pairwise separated by at least one and are all at least one (as in (1.2)), so their sum is at least $1 + 2 + \dots + Q = Q(Q+1)/2$.

On the other hand, each length $x_{i+j} - x_i$ is a sum of j consecutive gaps $x_{t+1} - x_t$, and for fixed j each gap occurs in at most j of these sums. So the lengths with a fixed j add up to at most jD , and all short lengths add up to at most $(1 + \dots + w)D = w(w+1)D/2$. Comparing the two bounds,

$$D \geq \frac{Q(Q+1)}{w(w+1)} \geq \frac{w}{w+1} \left(n - \frac{w+1}{2} \right)^2 \geq n^2 - \frac{n^2}{w+1} - n(w+1).$$

Finally $\sqrt{n} < w+1 \leq \sqrt{n} + 1$, so $D \geq n^2 - n^{3/2} - n^{3/2} - n \geq n^2 - 3n^{3/2}$. $\square$

For $d \geq 2$ the present argument leaves open the exact asymptotic behaviour of $\Delta_d(n)/n^2$, the least dimension in which the conjectured lower bound fails, and in particular the planar case.

ACKNOWLEDGMENTS

The author thanks Boon Suan Ho for helpful comments on an earlier draft of this manuscript.

ATTRIBUTION AND VERIFICATION SCOPE

The colex metric, its quantitative Gram reserves, and the fine and coarse incidence families F_A, G_A come from the first version of this paper [4]. Its clustered quadratic-residue ruler is retained with a free principal spacing parameter. The orthogonal-circle organization, the use of a single ruler for both local lengths and digits, and the derivative-based comparison of cross lengths are the modifications developed in this paper. The positive-semidefinite completion itself is elementary linear algebra.

This manuscript was developed with substantial AI assistance in mathematical exploration, proof engineering, source comparison, and writing. An AI-generated simplification of the construction and readability rewrite informed the revised construction and presentation, with permission to use it. The finite theorem stated here was checked in Lean 4 at the finite-proof source pin below. These checks do not constitute independent human proof or priority review. The concrete finite conclusion of [Theorem 1.1](#) has a Lean 4 proof in the [accompanying source bundle](#) (public source commit `f1604c3`), under the exact declaration `pass5_fixed_dimension_erdos_670`. It certifies an injective configuration, minimum distinct-point distance at least one, separation of genuinely distinct unordered edges, and the actual set diameter bound. Sixteen new source modules passed a fresh trust-zero replay, and a scoped build passed with cached upstream imports. Neither the Lean check nor this manuscript is an independent specialist proof or priority review. The supplementary rational and small-model checks alone are not proof certificates.

APPENDIX A. PROOF OF THE MACRO INPUT

We prove [Lemma 3.1](#), following the first version's macro estimates [4, Lemmas 2–3]. None of the cluster geometry of the main text is used here. The plan is as follows.

- (1) Compute the Gram matrix Γ of the *increments* $q_j - q_{j-1}$ that the colex distances would require ([Section A.1](#)).
- (2) Show that Γ is dominated by its tridiagonal part, and that this part contains two “reserves” of positivity: one large enough to pay for the shortening by $2\rho^2$, and one diagonal reserve ([Section A.2](#)). This proves part (i).

- (3) Use the diagonal reserve to bound the vectors F_A, G_A all at once, through their projections on the increments (Section A.3). This proves part (iii).

Throughout, $m \geq 4$ and K, ρ satisfy (3.2). Since $H_m \geq 1$, the harmonic gate implies $K \geq 16384 > 10$, as used below. Vectors $x \in \mathbb{R}^{m-1}$ are indexed $x_1, \dots, x_{m-1}$, and e_A ($0 \leq A < m$) denotes the standard basis of $\mathbb{R}^m$.

A.1. The increment Gram matrix. Let ∂ be the $(m-1) \times m$ matrix whose j -th row is $e_{j-1}^\top - e_j^\top$ ($1 \leq j < m$). For a symmetric $m \times m$ matrix $\mathbf{D}$ with zero diagonal, the matrix $-\frac{1}{2}\partial\mathbf{D}\partial^\top$ is the Gram matrix that the increments must have: if points q_A satisfy $\|q_A - q_B\|^2 = \mathbf{D}_{AB}$, then $\langle q_i - q_{i-1}, q_j - q_{j-1} \rangle = (-\frac{1}{2}\partial\mathbf{D}\partial^\top)_{ij}$, by the polarization identity. This is Schoenberg's Euclidean-distance criterion in consecutive-increment coordinates [5, Theorem 1].

Let $\mathbf{D}$ have entries D_{AB}^2 off the diagonal, put $\Gamma = -\frac{1}{2}\partial\mathbf{D}\partial^\top$, and write

$$D_j = D_{j-1,j} = K + \frac{j(j+1)}{2} \quad (1 \leq j < m)$$

for the lengths of the consecutive macro edges. Since $D_{j-1,j+1} = D_j + j$ and $D_{j,j+1} = D_j + j + 1$, a direct computation gives

$$(A.1) \quad \Gamma_{jj} = D_j^2, \quad \Gamma_{j,j+1} = -c_j, \quad \text{where } c_j = \frac{1}{2}(D_j + 1)^2 + j.$$

If $i \leq j-2$, the four lengths $D_{i-1,j-1}, D_{i-1,j}, D_{i,j-1}, D_{ij}$ have the form $\alpha, \beta, \alpha+1, \beta+1$ with $\beta - \alpha = j-1$, and therefore $\Gamma_{ij} = -(j-1)$. In other words, $\Gamma_{ij} = -(\max\{i, j\} - 1)$ whenever $|i - j| \geq 2$.

A.2. Two reserves of positivity. Split $\Gamma = \mathbf{B} - \mathbf{N}$, where the *band* $\mathbf{B}$ keeps the diagonal and the two neighbouring diagonals of Γ , and the *far part* $\mathbf{N}$ has entries $\max\{i, j\} - 1$ for $|i - j| \geq 2$ and zero otherwise. Completing squares in $-2c_j x_j x_{j+1}$ gives

$$(A.2) \quad \mathbf{B}[x] = \sum_{j=1}^{m-2} c_j (x_j - x_{j+1})^2 + \sum_{j=1}^{m-1} \alpha_j x_j^2 + c_{m-1} x_{m-1}^2,$$

where c_{m-1} is given by the same formula as the other c_j , $\alpha_j = D_j^2 - c_j - c_{j-1}$ with $c_0 = 0$, and explicitly

$$\alpha_1 = \frac{K^2}{2} - 2, \quad \alpha_2 = -4, \quad \alpha_j = (j-2)K + \frac{j^3}{2} - j^2 - 2j \quad (j \geq 3).$$

The band dominates a diagonal form. Define $\Omega = \text{diag}(\omega_1, \dots, \omega_{m-1})$ by

$$\omega_1 = \omega_2 = \frac{K^2}{24}, \quad \omega_j = \frac{Kj + j^3}{24} \quad (j \geq 3).$$

We claim $\mathbf{B} \succeq \Omega$. The terms of (A.2) involving only x_1, x_2 are $c_1(u-v)^2 + \alpha_1 u^2 - 4v^2$, with $u = x_1, v = x_2$. Since $c_1, \alpha_1 \geq K^2/4$ and $(u-v)^2 + u^2 \geq (u^2 + v^2)/3$,

$$c_1(u-v)^2 + \alpha_1 u^2 - 4v^2 \geq \frac{K^2}{12}(u^2 + v^2) - 4v^2 \geq \frac{K^2}{24}(u^2 + v^2)$$

for $K \geq 10$. For $j \geq 3$ we have $\alpha_j \geq \omega_j$, because

$$24(\alpha_j - \omega_j) = (23j - 48)K + 11j^3 - 24j^2 - 48j,$$

which is positive at $j = 3$ (it equals $21K - 63$), and has both terms nonnegative for $j \geq 4$. All remaining terms of (A.2) are nonnegative.

The far part is small. Put $\sigma_0 = \sum_j \omega_j^{-1}$ and $\sigma_2 = \sum_j j^2 \omega_j^{-1}$. For $K \geq 10$,

$$\sigma_0 \leq \frac{48}{K^2} + \frac{24H_m}{K} \leq \frac{29H_m}{K}, \quad \sigma_2 \leq \frac{120}{K^2} + 24H_m \leq 26H_m.$$

With $b_0 = \sum_j |x_j|$ and $b_1 = \sum_j j|x_j|$ we have $|\mathbf{N}[x]| \leq \sum_{i,j} \max\{i, j\} |x_i| |x_j| \leq 2b_0 b_1$, while weighted Cauchy–Schwarz gives $b_0^2 \leq \sigma_0 \Omega[x]$ and $b_1^2 \leq \sigma_2 \Omega[x]$. Therefore

$$(A.3) \quad |\mathbf{N}[x]| \leq 2\sqrt{\sigma_0 \sigma_2} \Omega[x] \leq \frac{\sqrt{754}}{64} \Omega[x] \leq \frac{1}{2} \Omega[x] \leq \frac{1}{2} \mathbf{B}[x],$$

using $K \geq 16384H_m^2$ (so that $\sqrt{29 \cdot 26} H_m / \sqrt{K} \leq \sqrt{754}/128$) and $754 < 1024$. Hence

$$\Gamma \succeq \frac{1}{2} \mathbf{B}.$$

First reserve: a path energy. Let Π be the quadratic form

$$\Pi[x] = D_1^2 x_1^2 + \sum_{j=1}^{m-2} D_j^2 (x_j - x_{j+1})^2 + D_{m-1}^2 x_{m-1}^2.$$

In (A.2), bound $-4x_2^2 \geq -8x_1^2 - 8(x_2 - x_1)^2$. Since $\alpha_1 - 8 \geq D_1^2/4$, $c_1 - 8 \geq D_1^2/4$, $c_j \geq D_j^2/4$ for all j , and $\alpha_j \geq 0$ for $j \geq 3$, this proves

$$(A.4) \quad \mathbf{B} \succeq \frac{1}{4} \Pi.$$

Second reserve: a diagonal. For every j ,

$$(A.5) \quad D_j^2 \leq 36(K+m)\omega_j, \quad \text{hence} \quad \mathbf{B} \succeq \Omega \succeq \frac{\text{diag}(D_1^2, \dots, D_{m-1}^2)}{36(K+m)}.$$

For $j = 1, 2$ the first inequality is immediate. For $j \geq 3$, use $D_j \leq K + j^2 \leq (K+m)j$ to get the stronger bound $D_j^2 \leq (K+j^2)(K+m)j = (K+m)(Kj + j^3)$.

Paying for the shortening. Shortening every squared distance by $2\rho^2$ replaces $\mathbf{D}$ by $\mathbf{D}_\rho$, with entries $D_{AB}^2 - 2\rho^2$ off the diagonal. Since the rows of ∂ sum to zero, the new increment Gram matrix is

$$\Gamma_\rho = -\frac{1}{2} \partial \mathbf{D}_\rho \partial^\top = \Gamma - \rho^2 \partial \partial^\top.$$

Now $\partial \partial^\top[x] = x_1^2 + \sum_j (x_j - x_{j+1})^2 + x_{m-1}^2 \leq \Pi[x]/K^2$, because every $D_j \geq K$. As $\rho \leq K/4$, the subtraction costs at most $\Pi/16 \preceq \mathbf{B}/4$, by (A.4). Combining this with $\Gamma \succeq \mathbf{B}/2$ and the two reserves,

$$(A.6) \quad \Gamma_\rho \succeq \frac{1}{4} \mathbf{B} \succeq \frac{1}{16} \Pi \succ 0, \quad \Gamma_\rho \succeq \frac{\text{diag}(D_1^2, \dots, D_{m-1}^2)}{144(K+m)}.$$

Here $\Pi \succ 0$ because $\Pi \succeq K^2 \partial \partial^\top$ and ∂ has full row rank.

Proof of part (i). Since $\Gamma_\rho \succ 0$, we may write $\Gamma_\rho = \mathbf{V}^\top \mathbf{V}$ for an invertible $(m-1) \times (m-1)$ matrix $\mathbf{V}$ with columns $v_1, \dots, v_{m-1}$ (for instance, by Cholesky factorization). Put $q_0 = 0$ and $q_A = v_1 + \dots + v_A$. For $A < B$ let $u_{AB} = \sum_{j=A+1}^B e_j \in \mathbb{R}^{m-1}$; then $\partial^\top u_{AB} = e_A - e_B$, and so

$$\|q_B - q_A\|^2 = \Gamma_\rho[u_{AB}] = -\frac{1}{2} (e_A - e_B)^\top \mathbf{D}_\rho (e_A - e_B) = D_{AB}^2 - 2\rho^2.$$

The increments $v_j = q_j - q_{j-1}$ are linearly independent, so the points q_A are affinely independent.

A.3. Bounding all projections at once. Let $Y_0, \dots, Y_{m-1} \in \mathbb{R}^{m-1}$ be vectors, and record their projections on the increments in the $(m-1) \times m$ matrix

$$Z_{jA} = \langle q_j - q_{j-1}, Y_A \rangle, \quad \text{that is,} \quad Z = \mathbf{V}^\top Y.$$

As $\mathbf{V}$ is invertible, Z determines Y , and $Y^\top Y = Z^\top (\mathbf{V}^\top \mathbf{V})^{-1} Z = Z^\top \Gamma_\rho^{-1} Z$. Writing $\mathbf{P} = \text{diag}(D_1, \dots, D_{m-1})$, the second inequality in (A.6) gives $\Gamma_\rho^{-1} \preceq 144(K+m)\mathbf{P}^{-2}$, and hence

$$(A.7) \quad \|Y\|_{\text{op}} \leq 12\sqrt{K+m} \|\mathbf{P}^{-1} Z\|_{\text{op}}.$$

So it suffices to show that the projection matrices of F and G , normalized by $\mathbf{P}^{-1}$, have bounded operator norm.

Taking consecutive differences of the defining equations (3.4) (with the convention that the right-hand sides vanish for $J = A$) gives, for $1 \leq j < m$ and $0 \leq A < m$,

$$\begin{aligned} Z_{jA}^F &= D_j \mathbf{1}_{A=j} - \mathbf{1}_{A>j}, \\ Z_{jA}^G &= -D_j \mathbf{1}_{A=j-1} - (j-1) \mathbf{1}_{A<j-1}. \end{aligned}$$

For example, for $A > j$ we get $Z_{jA}^F = D_{j-1,A} - D_{jA} = -1$, because the colex labels of $\{j-1, A\}$ and $\{j, A\}$ differ by one. The columns F_0 and G_{m-1} vanish. Delete them, and index the remaining columns by $1, \dots, m-1$ (column A of Z^F , and column $A-1$ of Z^G , become column A). The two projection matrices become

$$Z_{\text{fine}} = P - E_+, \quad Z_{\text{coarse}} = -(P + E_-),$$

where $(E_+)_{ij} = \mathbf{1}_{i<j}$ and $(E_-)_{ij} = (i-1)\mathbf{1}_{j<i}$.

For the first matrix, the Frobenius norm gives $\|P^{-1}E_+\|_{\text{op}} \leq m/K \leq 1$, as all entries of $P^{-1}E_+$ are at most $1/K$. For the second,

$$0 \leq (P^{-1}E_-)_{ij} = \frac{i-1}{D_i} \mathbf{1}_{j<i} \leq \frac{2}{i} \mathbf{1}_{j<i}$$

since $D_i \geq i(i+1)/2$. The finite Hardy matrix $\mathcal{H}_{ij} = i^{-1}\mathbf{1}_{j<i}$ has operator norm at most 2 by the weighted Schur test [6, 7]. For completeness, take the weights $w_j = j^{-1/2}$; by comparison with integrals,

$$\sum_{j<i} \frac{w_j}{i} \leq 2w_i, \quad \sum_{i>j} \frac{w_i}{i} \leq 2w_j.$$

For any real vector x , Cauchy–Schwarz with these weights then gives

$$\sum_i \left(\sum_j \mathcal{H}_{ij} x_j \right)^2 \leq \sum_i \left(\sum_j \mathcal{H}_{ij} w_j \right) \left(\sum_j \mathcal{H}_{ij} \frac{x_j^2}{w_j} \right) \leq \sum_j \frac{x_j^2}{w_j} \sum_i 2w_i \mathcal{H}_{ij} \leq 4 \sum_j x_j^2.$$

A matrix with nonnegative entries bounded by those of $2\mathcal{H}$ has operator norm at most $2\|\mathcal{H}\|_{\text{op}}$ (apply it to $|x|$), so $\|P^{-1}E_-\|_{\text{op}} \leq 4$.

Thus $\|P^{-1}Z_{\text{fine}}\|_{\text{op}} \leq 2$ and $\|P^{-1}Z_{\text{coarse}}\|_{\text{op}} \leq 5$, and (A.7) gives $\|F\|_{\text{op}} \leq 24\sqrt{K+m}$ and $\|G\|_{\text{op}} \leq 60\sqrt{K+m}$; restoring the zero columns does not change the norms. This proves (3.5) and completes the proof of Lemma 3.1. $\square$

REFERENCES

- [1] P. Erdős, *Some unsolved problems*, in *Combinatorics, Geometry and Probability: A Tribute to Paul Erdős*, B. Bollobás and A. Thomason (eds.), Cambridge University Press, 1997, pp. 1–10, Problem 20. [doi:10.1017/CBO9780511662034.004](https://doi.org/10.1017/CBO9780511662034.004).
- [2] P. Erdős and P. Turán, *On a problem of Sidon in additive number theory, and on some related problems*, J. London Math. Soc. **16** (1941), 212–215. [doi:10.1112/jlms/s1-16.4.212](https://doi.org/10.1112/jlms/s1-16.4.212).
- [3] Boon Suan Ho, *Erdős’s diameter conjecture for separated distances fails in high dimensions*, 2026, [arXiv:2604.15305v1](https://arxiv.org/abs/2604.15305v1).
- [4] J. Tripodo, *Separated Euclidean distances with diameter below $0.74n^2$ in a fixed dimension*, research manuscript, 12 October 2026. Public source snapshot 1e73a12, [jjtripodo-lgtm/erdos-670-fixed-dimension, paper/fixed_dimension_670.tex](https://github.com/jjtripodo-lgtm/erdos-670-fixed-dimension/paper/fixed_dimension_670.tex).
- [5] I. J. Schoenberg, *Remarks to Maurice Fréchet’s article “Sur la définition axiomatique d’une classe d’espace distanciés vectoriellement applicable sur l’espace de Hilbert”*, Ann. of Math. (2) **36** (1935), 724–732. [doi:10.2307/1968654](https://doi.org/10.2307/1968654).
- [6] I. Schur, *Bemerkungen zur Theorie der beschränkten Bilinearformen mit unendlich vielen Veränderlichen*, J. Reine Angew. Math. **140** (1911), 1–28. [doi:10.1515/crll.1911.140.1](https://doi.org/10.1515/crll.1911.140.1).
- [7] G. Sinnamon, *Schur’s lemma and best constants in weighted norm inequalities*, Le Matematiche **57** (2002), fasc. II, 185–204. <https://lematematiche.dmi.unict.it/index.php/lematematiche/article/view/207>.
- [8] P. L. Robinson, *Julia operators and Halmos dilations*, arXiv:1803.09329v1, 2018. <https://arxiv.org/abs/1803.09329v1>.
- [9] P. Erdős, *On sets of distances of n points in Euclidean space*, Publ. Math. Inst. Hungar. Acad. Sci. **5** (1960), 165–169. https://users.renyi.hu/~p_erdos/1960-08.pdf.